International Journal of Electrical, Computing Engineering and Communication (IJECC)

Vol. 1, Issue. 1, January – 2015 *ISSN (Online): XXXX-XXXX*

A Location Monitoring System for WSN by Preserving Privacy

[1]T. Manikandan,
Assistant Professor – Department of Computer Science & Engineering,
Fatima Michael College of Engineering & Technology, Madurai, INDIA.
(engr_manikandan@yahoo.co.in)

Abstract –

Advances in sensor networking and location tracking technology enable location - based applications but they also create significant privacy risks. Privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user's decision to release data. However, privacy policies require user interaction and offer little protection from malicious service providers. Protection of user's privacy has been a central issue for location-based services (LBSs).

Here, to strike a balance between the location privacy and QoS, we present two location anonymization algorithms, namely, resource and quality-aware algorithms, that aim to enable the system to provide high-quality location monitoring services for system users, while preserving personal location privacy. The system is evaluated through some simulated experiments, whereas the results show that our system provides high-quality location monitoring services for system users and guarantees the location privacy of the monitored persons.

Keywords - Location privacy, QOS, k-anonymity, location monitoring system, location based services, aggregate query processing.

I. INTRODUCTION

Sensor networks promise to have a significant commercial impact by providing strategic and timely data to new classes of realtime monitoring applications. Providing privacy in sensor networks is complicated by the fact that sensor networks consist of low-cost radio devices that employ readily available, standardized wireless communication technologies. Privacy may be defined as the guarantee that information, in its general sense, is observable or decipherable by only those who are intentionally meant to observe or decipher it.

The phrase "in its general sense" is meant to imply that there may be types of information besides the message content that are associated with a message transmission. Many of the privacy techniques employed in general network scenarios are not appropriate for protecting the source location in a sensor network. This is partially due to the fact that the problems are different, and partially due to the fact that many of the methods introduce overhead which is too burdensome for sensor networks.

In the context of LBSs, the K-anonymity concept translates as follows: Given a query, guarantee that an attack based on the query location cannot identify the query source with probability larger than 1=K among other K/1 users. Most of the existing work adopts the framework in Fig 1.

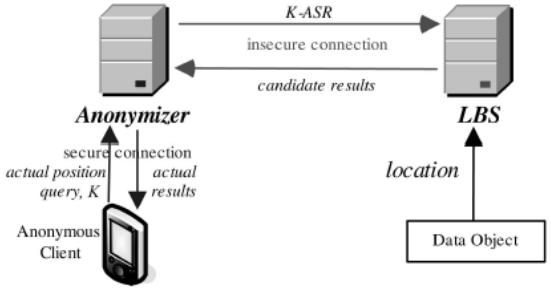

Fig 1 Example for spatial K-Anonymity

In this framework, a user sends his location and query to the anonymizer through a secure connection. The anonymizer removes the ID of the user and transforms his location through a technique called cloaking. Cloaking hides the actual location by a K-anonymizing spatial region (K-ASR or ASR), which is an area that encloses the client that issued the query, and at least K/1 other users.

The anonymizer then sends the ASR to the LBS, which returns to the anonymizer a set of candidate results that satisfy the query condition for any possible point in the ASR. The LBS may be compromised that is, an adversary may have complete knowledge of all queries received by the LBS.

II. SYSTEM MODEL

The architecture of our system consists of three major entities such as, sensor nodes, server, and system users. It is shown in fig2.

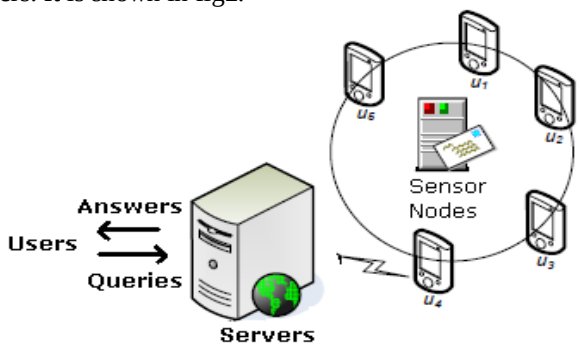

Fig 2 System Architecture

The sensor nodes are used to find the total number of objects in each sensing area, the sensor nodes are used where as, it converts its sensing area into a clocked area A. Whereas, each clocked area A have atleast k objects. So, periodically, it updates the server about the number of objects located in A as aggregate location information. But, in our system, the type of network topology is not taken into account since our system requires only a communication path. This path lies between all the sensor nodes and the centralized server through a distributed tree. Each sensor node is also aware of its location and sensing area.

A common server is used to collect the reports from the sensor nodes. Later, spatial histograms are used to find the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Practically, the value of anonymized level k can be changed to any value only by the administrator. This can be achieved by sending a message to all the sensor nodes regarding the new anonymized level k.

The system users are divided into two categories namely the normal users and the administrators. Range queries are issued by the normal users as well as the administrators through corresponding server or the sensor nodes. Later, the server answers the queries by means of spatial histogram.

Privacy model: A framework is introduced such that, the sensor nodes constitute a trusted zone. It is defined in our algorithm and each sensor node communicates with each other through a secure network channel. This avoids internal network attacks.

The concept of k-anonymity was originally introduced in the context of relational data privacy. It addresses the question of "how a data holder can release its private data with guarantees that the individual subjects of the data cannot be identified whereas the data remain practically useful". For instance, a medical institution may want to release a table of medical records with the names of the individuals replaced with dummy identifiers.

However, some set of attributes can still lead to identity breaches. These attributes are referred to as the quasi-identifier. For instance, the combination of birth date, zip code, and gender attributes in the disclosed table can uniquely determine an individual. By joining such a medical record table with some publicly available information source like a voters list table, the medical information can be easily linked to individuals. k-anonymity prevents such a privacy breach by ensuring that each individual record can only be released if there are at least k -1 distinct individuals whose associated records are indistinguishable from the former in terms of their quasi-identifier values.

III. LOCATION ANONYMIZATION ALGORITHMS

In order to capture varying location privacy requirements and ensure different levels of service quality, each client specifies its anonymity level (k value), spatial tolerance, and temporal tolerance. The main task of a location anonymity server is to transform each message received from clients into a new message that can be safely (k-anonymity) forwarded to the LBS provider.

The key idea that underlies the location k-anonymity model is twofold. First, a given degree of location anonymity can be maintained, regardless of population density, by decreasing the location accuracy through enlarging the exposed spatial area such that there are other k – 1 clients present in the same spatial area.

Sensor nodes reports their k-anonymous aggregate locations to the server for every reporting period. For this, two algorithms namely, resource and quality aware location anonymization algorithms are used.

A. The Resource Aware Algorithm

In general, the algorithm has three steps. They are :

- Broadcast Step
- Clocked Area Step
- Validation Step

Broadcast Step

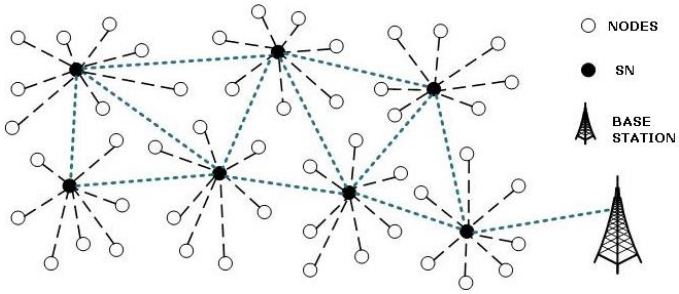

Fig 3 Broadcast Step

In fig3, each sensor node is surrounded by a number of wireless nodes. Here, sensor nodes are used to find the adequate number of objects by broadcasting in a frequent interval of time. The same is used to comptute a clocked area. If an neighbour node have not found any adequent number of objects, then the sensor node forwards its received messages.

This operation reduces the cost of communication. This process continues, until each node finds an adequent number of objects. After that, during the reporting period, each sensor node sends a message to its neighbours where the message includes its identity, sensing area, and the number of objects located in its sensing area.

Clocked Area Step

In this step, each sensor node must satisfy some k-anonymity privacy requirement. For that, it blurs its sensing area into a cloaked area that includes at least k objects. Then, depending upon the number of nodes surrounded and the distance between them, an MBR is drawn as shown in fig 4.

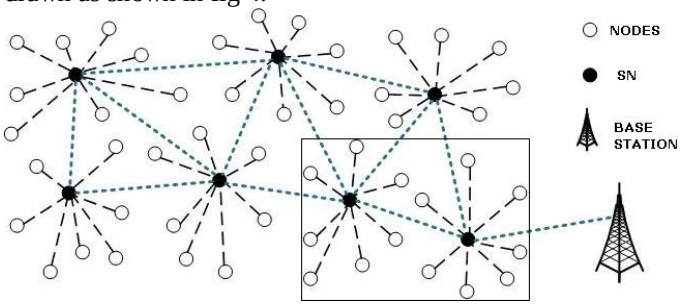

Fig 4 Forming minimum bounding rectangle

Ususally, a greedy approach is used to find a clocked area based on the information stored. This approach minimizes the computational cost. Finally, a minimum bounding rectangle (MBR) is drawn which covers the sensor nodes S and the total number of objects in S(N). MBR's are manipulated by most of the database management systems efficiently. So this method is adopted by various query processing algorithms.

Validation Step

The objective of this step is to avoid reporting aggregate locations with a containment relationship to the server. As this step ensures that no aggregate location with the containment relationship is reported to the server, the adversary cannot obtain any deterministic information from the aggregate locations. Since the server receives an aggregate location from each sensor node for every reporting period, it cannot tell whether any containment relationship takes place among the actual aggregate locations of the sensor nodes.

B. The Quality Aware Algorithm

After the completion of all the steps in the resource aware algorithm, the clocked area computed by it is taken as an initial solution for this algorithm. Also, this quality aware algorithm refines it until the cloaked area reaches the minimal possible area. But still it satisfies the k-anonymity privacy requirement.

This can be achieved by means of the extra communication between other peers. Here instead of the clocked area step in the resource aware algorithm, a minimal cloaked area is initialized by the quality aware algorithm as an input initial solution. Similar to resource aware, this algorithm also has three steps.

Step 1: The search space step.

All the nodes in the wireless sensor network will be in some mobility. Thus in a frequent interval of time, some nodes leaves the sensing area, whereas, some other nodes will enter into the sensing area. Similarly, the network also has a large number of sensor nodes. This makes too costly for the sensor node m to gather the information of all the sensor nodes to compute its minimal cloaked area.

So, a search space S is determined to minimize the communication and computational cost. This can be achieved by taking the cloaked area computed by the resource-aware algorithm as the initial step. So, whatever the nodes outside S will cannot be part of the minimal cloaked area.

Step 2: The minimal cloaked area step.

Here, instead of clocked area in resource aware algorithm, a minimal clocked area is computed for the sensor node m. The input for this step is obtained by taking a set of peers residing in the search space S.

In our model, the search space step already prunes the entire system space into S. So, in order to obtain the minimal clocked area, we have to search all the possible combinations of these peers. So, mostly this could still be costly.

Step 3: The validation step.

The algorithm to find the validation is also the same as in the resource aware algorithm.

IV. EXPERIMENTAL RESULTS

A

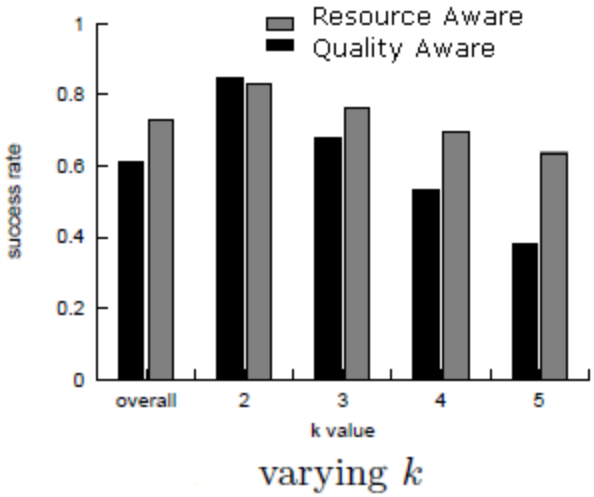

Fig 5 Success rate vs K Value

Success rate is an important measure for evaluating the effectiveness of the proposed quality aware algorithm. Concretely, the primary goal of the quality aware algorithm is to minimize the clocked area. Because, each clocked area is identified by the corresponding sensor nodes and then the same is reported to the server such that, it becomes difficult for the attacker model error.

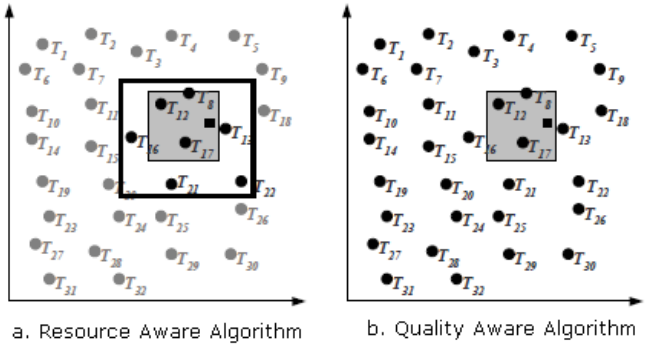

Fig 6 Minimal Clocked Area

The success rate is also changes with respect to the total number of objects present in the sensing area. When the total number of objects increases, forming minimum bounding rectangle is easier since the communication cost of the quality aware algorithm is less when compared to the resource aware algorithm.

V. CONCLUSION

While location-based services become essential in supporting a broad area of applications (navigation systems, emergency services, etc), new privacy concerns arise for LBS users (e.g. in the near future GSM phones will be equipped with a clipper chip that accurately tracks users).This paper introduces two algorithms to preserve the location privacy of the System Users. Each sensor nodes finds an aggregate location which is a clocked area A and the total number of objects present in the sensing area.

Experimental evaluation studies the algorithms by changing both the total number of users and the k-anonymity level. The results reveal the accuracy level to another 15% when using the resource aware algorithm.

REFERENCES

[1] R. Cheng, Y. Zhang, E. Bertino and S.Prabhakar (2008) 'Perserving user location privacy in mobile data management infrastructures' Intl. Workshop on privacy Enhancing Technologies, pages 393 – 412.

[2] C-Y. Chow and M..F. Mokbel (2007) 'Enabling Private Continuous Queries for Revealed User Locations' Proc. of SSTD, pages 258 – 275.

[3] G. Ghinita, P. Kalnis, and S. Skiadopoulos (2007) 'PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems' Proc. of Int. Conference on WWW, pages 371–380.

[4] M.F. Mokbel, C.Y. Chow and W.G. Aref (2006) 'The New Casper: Query Processing for Location Services without Compromising Privacy' Proc of VLDB.

[5] B. Gedik and L. Liu (2005) 'Location privacy in Mobile Systems: A personalized Anonymization Model' Proc. of ICDCS, pages 620-629.

[6] L. Sweeney (2006) 'k-Anonymity: A Model for Protecting Privacy' Int. J. of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5):557.

[7] E. Kaasinen (2004) 'User Needs for Location - Aware mobile services' Personal and Ubiquitous computing, 7(1): 70-79.

[8] M. Gruteser and X. Liu (2006) 'Protecting Privacy in Continuous Location-Tracking Applications' IEEE Security and Privacy, 2(2):28–34

[9] Claudio Bettini, X. Sean Wang and Sushil Jajodia (2005) 'Protecting privacy against location - based personal identification' In Proc. of the 2nd workshop on Secure Data Management (SDM), volume 3674 of LNCS, pages 185–199, Springer.

[10] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh (2005) 'An anonymous communication technique using dummies for location-based services' In Proc. of the International Conference on Pervasive Services (ICPS), pages 88–97. IEEE Computer Society.